



TRUSTED INFORMATION SYSTEMS, INC.

Building a World of Trust™

March 13, 1997

STEPHEN T. WALKER  
PRESIDENT

Ms. Nancy Crowe  
Regulatory Policy Division, Room 2705  
Bureau of Export Administration  
Department of Commerce  
14<sup>th</sup> Street and Pennsylvania Avenue, N.W.  
Washington, DC 20230

Re: Additional Comments On "Encryption Items  
Transferred from the U.S. Munitions List to the  
Commerce Control List"

Dear Ms. Crowe:

Having recently performed an in-depth evaluation of "Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List" (61 Federal Register 68572-68587)(the "Interim Rules"), Trusted Information Systems, Inc. ("TIS") submits these Additional Comments to supplement the comments filed by TIS on February 11, 1997.

TIS regrets not having submitted these comments prior to the expiration of the comment period stated in the Interim Rules, but the information contained herein did not become apparent until after TIS undertook detailed discussions regarding the development of actual products intended to comply with the new criteria.

TIS believes the provisions of Supplement No. 4 to Part 742 – Key Escrow or Key Recovery Products Criteria – contains inconsistencies that will lead product developers to produce products that may meet the letter of the rule, but will not be approved for export. In addition, the cost and delay associated with correcting this situation will ultimately delay the widespread acceptance and use of key recovery products and services.

Circa 1995 there were three "product criteria" addressing (i) two-sided recovery, (ii) interoperability, and (iii) tamper-resistance. The Interim Rules combined these into two product criteria: (i) a two-part "interoperability" criterion (Section 6), and (ii) tamper-resistance (Section 7). The consolidation resulted in rendering the tamper-resistance requirements unenforceable. Therefore, product developers face substantial—and potentially costly—uncertainty regarding exportable product design.

The three original criteria required each side of a communication to verify the other's key recovery information before decryption could occur. This meant that two key-recovery products formed a "closed system" where tampering with, or bypassing, key recovery features would be detectable—and detected. Tamper-resistance would be enforced in both the product (by controlling how input is processed) *and the key recovery information generated by the product (the output)*.

3060 Washington Road (Rt. 97), Glenwood, Maryland 21738

(301) 854-6889 • www.tis.com • (301) 854-5363 (F)

The new Section 6 of Supplement No. 4 part 742 (Interoperability Feature) is internally inconsistent with respect to the Section 7 provisions regarding tampering with, or otherwise bypassing or disabling, key recovery features.

If a key recovery product is required to ensure the key recovery mechanism has not been tampered with in order for the product to function, that product will not function if the key recovery information is not present (per Sections 6(i) and 7). By contrast, the interoperability provision states that a message may be processed by a key recovery product without the key recovery information (when it is "interoperating" per Section 6(ii)). TIS has encountered great difficulty attempting to reconcile these requirements.


To further clarify the problem created by this discrepancy, consider that one could legally tamper with the data after it leaves the tamper resistant product, but before it is transmitted, without violating the tamper resistance requirements of Section 7. It should be noted that a message generated by a product with bypassed or tampered-with key recovery features will look exactly like a message generated by a non-recovery product, both to a law enforcement interception, and to another product receiving the message. Put another way, a message generated in such a manner would "appear" to another key recovery product to be a message generated by a non-key recovery product, which is permitted by the Interim Rules. Accordingly, the tamper-resistance provisions cannot be enforced, and Section 7 of Supplement No. 4 is effectively rendered meaningless. Conversely, if Section 7 is to be valid, Section 6 is fatally flawed.

It is very easy – even trivial – to tamper with data (e.g., removing key recovery information) prior to sending it, but after it is generated by a key recovery product. However, if the recipient is required to verify that the key recovery information is intact and unmodified prior to decryption, and as a condition for decryption (i.e., the product won't decrypt unless the check verifies) the system, as a whole, can ensure that key recovery information will always be available.

In conclusion, the interoperability capability and tamper resistance requirements specified in the Interim Rule are inherently inconsistent and will prevent TIS and others from developing and deploying fully compliant key recovery products. In light of the forgoing, TIS requests that clarifying revisions be made to address this inconsistency prior to, or as a part of, the promulgation of final, permanent regulations.

Again, thank you for the opportunity to provide these Additional Comments on the Interim Rule. If you have any questions regarding this submission, or if you require any additional information, please contact Joan Winston at (703)356-2225 ext. 111 or Ken Mendelson at (301) 854-5348.

Sincerely,



Stephen T. Walker